Fantasio

Zeste de savoir

Faire tourner un vieux jeu nativement sour Windows

7 septembre 2020

Table des matières

Bonjour à tous! Aujourd'hui je vais vous parler d'une petite expérience que j'ai faite pour essayer de faire marcher un vieux jeu

Il y a quelques temps, j'ai retrouvé sur une des mes vieilles machines Ford Racing 2 , et je me suis mis en tête de le relancer pour retrouver les sensations de l'époque.

1. Comment faire marcher un vieux jeu ?

Comme je disais, me voilà en possession d'un dossier contenant le jeu et la première chose que je teste, c'est bien sûr d'essayer de le lancer directement. L'introduction marche, mais une fois passée, le jeu plante avec un message d'erreur.

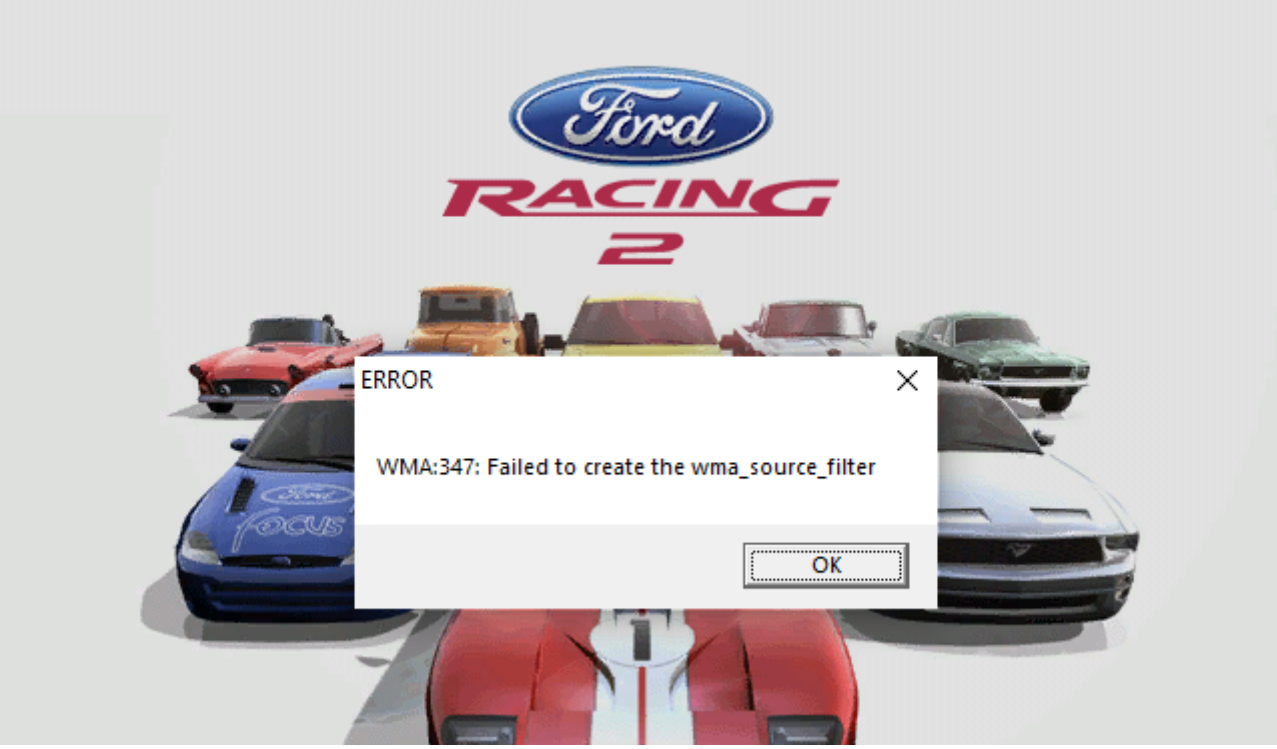

FIGURE 1.1. – Une petite erreur bien désagréable

Une petite recherche me mène rapidement sur un forum qui propose un binaire patché du jeu qui évite cette erreur (je ne mets pas le lien car il est un peu shady), mais je n'ai pas spécialement envie de faire tourner ça chez moi.

A partir de là, j'ai trois possibilités:

— Utiliser une VM de Windows pour faire tourner le jeu. Je n'en ai pas d'installée sur ma machine et j'avais un peu la flemme de trouver une image donc j'écarte ça.
— Utiliser Wine avec Linux, qui arrive à faire des miracles sur un certain nombre de jeux. En l'occurrence j'étais sous Windows et utiliser Linux impliquait de redémarrer mon ordinateur. Par flemme j'écarte à nouveau cette option.
— Tenter de modifier le binaire pour éviter l'erreur, quitte à perdre en fonctionnalité. Vu que quelqu'un l'a visiblement déjà fait, il y a une chance pour que ça soit faisable. En plus, ça faisait un petit moment que je voulais me plonger dans le binaire d'un jeu, c'était donc l'occasion de m'y mettre!

Bon ce n'est pas la méthode que je recommanderais dans l'absolu, mais mon "moi" du moment s'est dit qu'il y avait une chance pour que ça se passe bien.

2. Patch du binaire

A partir de là, je lance Cutter , qui permet de désassembler et de modifier le binaire.

Une recherche rapide me permet de trouver le message d'erreur dans les chaînes de caractères. Cutter permet de chercher les références à cette adresse, ce qui me permet de trouver la fonction qui se sert de ce message.

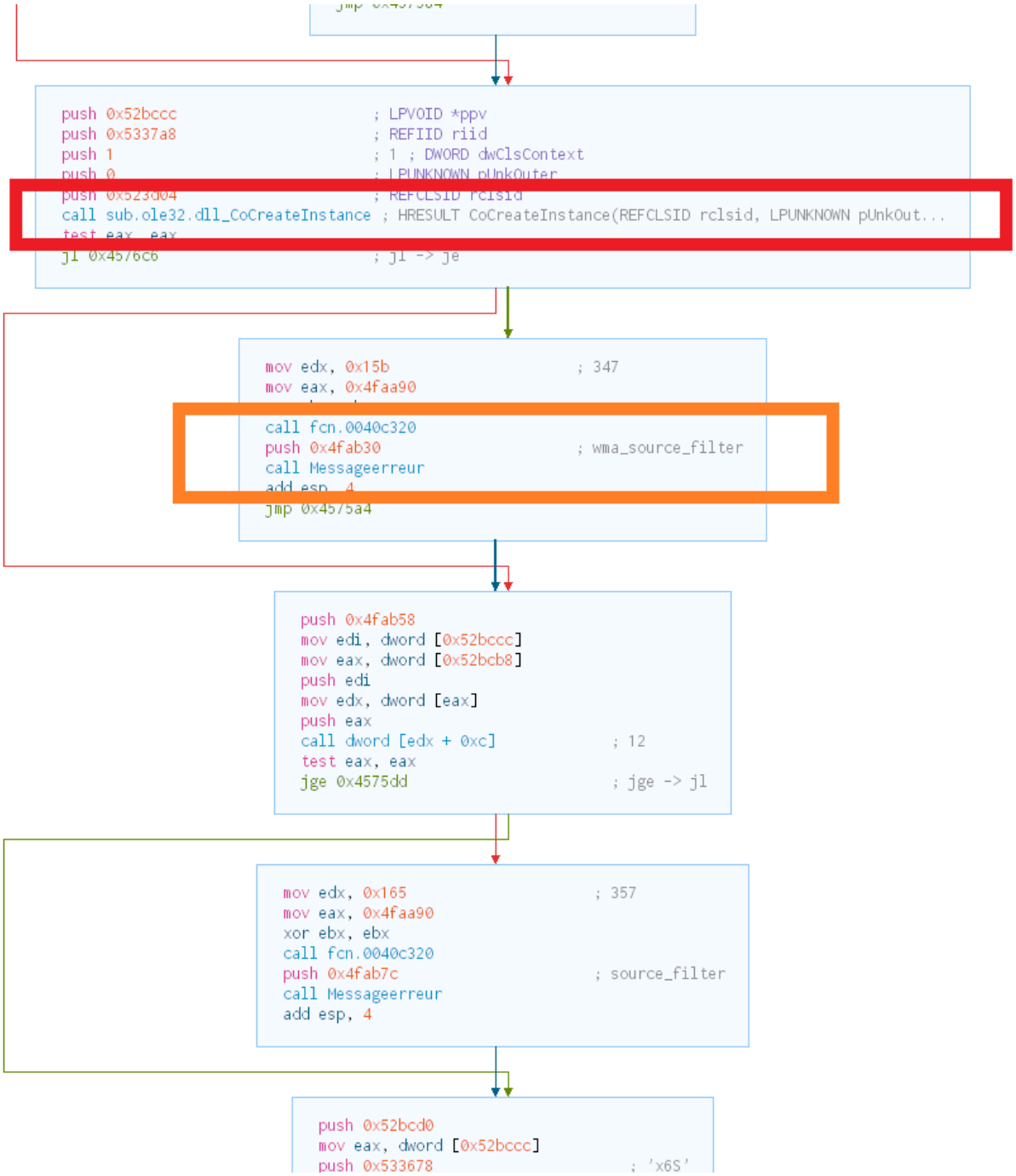

FIGURE 2.2. – La fonction qui déclenche l'erreur. En orange la référence à la chaîne de caractères. En rouge l'appel à la fonction CoCreateInstance qui retourne une erreur.

Je teste d'abord, sans trop y croire, d'inverser le test (présent après l'appel à *CoCreateInstance*) pour que l'exécution continue. Une nouvelle erreur apparaît, que j'essaie de faire disparaître de la même manière: cette fois, le programme crashe sans message d'erreur. Mauvaise méthode donc.

Deuxième essai: je localise les appels à cette fonction dans le reste du code. Coup de chance, elle n'est appelée qu'une seule fois ailleurs! Je neutralise cet appel (en le remplaçant par des NOP, l'instruction qui n'a pas d'effet). Je lance le jeu et… bingo! Il fonctionne à nouveau! Seul problème, la bande son du jeu n'est pas jouée, mais les bruitages sont toujours là. Je lance VLC avec la bande son et je peux enfin me lancer dans ma petite session nostalgie 🍊

FIGURE 2.3. – J'ai maintenant de quoi faire chauffer le bitume en 600 * 400

3. Bonus

Deux petites choses en bonus que j'ai pu trouver:

— La configuration du jeu est écrite dans le registre. Pour configurer le jeu il faut lancer un utilitaire fourni avec. Je trouve ça pas super malin mais ça m'a fait rire.
— Dans les chaînes de caractère du jeu j'ai trouvé des évocations à l'activation de cheats… Je vous avoue que ça me titille d'aller voir de quoi il s'agit 🍊

i

Petite anecdote sur la configuration dans le registre: à la base j'ai vu que je pouvais passer le jeu en Full HD, donc je me suis empressé de le faire. Sauf que je n'avais pas vu qu'il passait le jeu en couleur 16 bits, ce qui m'a empêché de relancer le jeu… et l'utilitaire aussi! J'ai du relancer le jeu avec Procmon pour comprendre où il allait chercher la config… La galère 🍊

Bilan des courses: le jeu marche!

Je vous avoue que je n'y croyais pas du tout au début et j'étais plus motivé par la curiosité qu'autre chose.

Si vous voulez bricoler vos jeux vous aussi sachez que:

— Ici, j'ai eu un sacré coup de bol qu'il n'y ait qu'un seul appel incompatible avec Windows 10. Honnêtement, je pense que ça tient du miracle.
— Un bon nombre de jeux plus récents sont protégés par des solutions qui rendent le reverse engineering **très** compliqué (par exemple Denuvo et VMProtect).
— Légalement, le reverse engineering tombe sous le coup de la loi française, et communiquer dessus encore plus. Ici, je m'appuie sur l'article L122–6-1 du Code la propriété intellectuelle qui me permet de le faire pour des raisons d'interopérabilité (et accessoirement le jeu est assez vieux donc je doute que l'éditeur essaie de poursuivre qui que ce soit de toute manière).